vogel—partner
RECHTSANWÄLTE

Infoblatt Corona-Virus und Home-Office

Datum:	9. April 2020
Betreff:	**Arbeits- und Datenschutzrecht**

Vorbemerkung:

Die Antworten sind als erste Orientierungshilfe für Arbeitgeber gedacht. Bei Einzelfragen im Hinblick auf die konkrete Situation Ihres Unternehmens sollte grundsätzlich anwaltlicher Rat eingeholt werden.

Ausgangssituation

In unseren ersten Infoblättern haben wir die drängendsten rechtlichen Fragen rund um die Reaktion auf das Corona-Virus beantwortet und u.a. darüber informiert, wie schnell und einvernehmlich Home-Office eingeführt werden kann (Stichwort: „*Kein Recht und keine Pflicht auf Home-Office*").

Die Einführung ist bei den meisten Mandanten inzwischen abgeschlossen – wie auch wir arbeitet aktuell jeder Zweite ganz oder teilweise im Home-Office. Nunmehr geht es um zahlreiche arbeits- und datenschutzrechtliche Folgefragen, die wir hier beispielhaft beantworten wollen:

Brauchen Sie eine Home-Office-Vereinbarung?

In der Regel ja. Durch das Arbeiten aus dem Home-Office ändern sich wesentliche Arbeitsvertragsinhalte, wie der Arbeitsort, die Erreichbarkeit und die Arbeitsmittel. Diese veränderten Bedingungen müssen neu geregelt werden.

Besteht ein Betriebsrat, so ist wegen der Vielzahl an mitbestimmungspflichtigen Themen der Abschluss einer Home-Office-Betriebsvereinbarung zu empfehlen. Diese hat den Vorteil, dass Sie unmittelbar und zwingend auf die Arbeitsverhältnisse einwirkt, deutlich leichter abänderbar und vom Anwendungsbereich des strengen AGB-Rechts ausgenommen ist.

Um diese Vereinbarungen nicht zu überfrachten, empfiehlt es sich, daneben wesentliche Rahmenbedingungen und Verhaltensregeln in einer unternehmensinternen Home-Office-Richtlinie zusammenzufassen. Auf diese sollte ggf. Bezug genommen werden.

Bei sämtlichen nachfolgenden Themen sind ggf. die Mitbestimmungsrechte des Betriebsrates zu beachten.

Und was muss in einer Home-Office-Vereinbarung geregelt werden?

Wir empfehlen Ihnen die folgenden The-

Büro Stuttgart
Königsbau-Passagen
Königstraße 26
D-70173 Stuttgart
Fon +49 711 24 83 95 200
Fax +49 711 24 83 95 205
info@vogel-partner.eu

Büro Karlsruhe
Technologiepark Karlsruhe
Emmy-Noether-Straße 17
D-76131 Karlsruhe
Fon +49 721 78 20 27 0
Fax +49 721 78 20 27 27
info@vogel-partner.eu

BW Bank Karlsruhe
IBAN: DE74 6005 0101 0002 7431 45
BIC-Code: SOLADEST600

Vogel & Partner Rechtsanwälte mbB
Sitz Karlsruhe – AG Mannheim PR 700160

www.vogel-partner.eu

men in einer Home-Office-Vereinbarung zu regeln:

- ***Arbeitsort***

Der Arbeitsort sollte in Kombination mit einer Versetzungsklausel konkret festgelegt werden.

Wird keine vertragliche Regelung über den Arbeitsort getroffen, kann der Arbeitgeber einerseits zwar über sein Weisungsrecht den Arbeitnehmer an unterschiedlichen Orten einsetzen. Andererseits hat er ihm im Fall einer betriebsbedingten Kündigung auch freie Arbeitsplätze an allen bestehenden Betriebsstätten anzubieten.

Im Falle alternierender Arbeit sowohl aus dem Home-Office als auch (ggf. an bestimmten Tagen) vor Ort im Betrieb sollte dies ebenfalls entsprechend vereinbart werden.

- ***Kontroll-/Zutrittsrecht***

Aus Gründen des Arbeits- und Datenschutzes sind Kontroll- und Zutrittsbefugnisse des Arbeitgebers unumgänglich. Dabei ist eine vertragliche Regelung des Zutrittsrechts des Arbeitsgebers zwingend, da wegen der mittelbar auch den Arbeitgeber bindenden, grundrechtlich geschützten Unverletzlichkeit der Wohnung nach Art. 13 Abs. 1 GG ein Betreten privater Wohnräume ohne Zustimmung des Arbeitnehmers nicht zulässig ist. Verweigert ein Arbeitnehmer nach allgemeiner Zustimmung ohne Sachgrund das Betreten der Wohnung, kann dies den Arbeitgeber im Einzelfall dazu berechtigen, die Tätigkeit im Home-Office durch Widerruf (s.u.) oder Änderungskündigung zu beenden.

Der Datenschutz erfordert einerseits, dass der Arbeitgeber als Verantwortlicher i.S.d. DSGVO auch im Home-Office „Herr der Daten" bleiben muss. Andererseits verlangt er ebenso, dass auch den Interessen des Arbeitnehmers angemessen Rechnung getragen wird. Hierbei sind abgestufte Kontrollmechanismen denkbar, in denen der Arbeitgeber beispielsweise zunächst Selbstauskünfte des Arbeitnehmers zu räumlichen Sicherheitsmaßnamen im Home-Office genügen lässt und ggf. nur in Stichproben oder bei Verdacht auf einen Verstoß eine Überprüfung durch den Arbeitgeber (im Beisein des betrieblichen Datenschutzbeauftragten) erfolgt.

- ***Lage der Arbeitszeiten und Erreichbarkeit***

Das Arbeitszeitgesetz gilt selbstverständlich auch für Tätigkeiten im Home-Office. Ihre Mitarbeiter müssen, auch wenn sie von zu Hause aus arbeiten, Höchstgrenzen, Pausenregelungen und Ruhezeiten einhalten. Der Arbeitgeber ist insofern Verantwortlicher und muss die entsprechenden Bestimmungen durchsetzen.

Praxistipp: Da die Überwachung der Mitarbeiter im Home-Office nur eingeschränkt möglich ist, empfehlen wir Ihnen als Arbeitgeber, Ihre Pflicht zur Dokumentation der täglichen Arbeitszeit daher auf den jeweiligen Mitarbeiter zu delegieren. Dann muss Ihr Mitarbeiter seine täglichen Arbeitszeiten, insbesondere wenn sie über die Acht-Stunden-Grenze hinausgehen, erfassen und Ihnen vorlegen. Als grobe Orientierung können auch Login- und Logout-Zeiten auf die betrieblichen IT-Systeme aus dem Home-Office heraus dienen, wobei deren Arbeitgeber-seitige Protokollierung und Überwachung dem

Arbeitnehmer zumindest transparent gemacht werden und in Unternehmen mit Betriebsrat auch mit diesem abgestimmt werden müssen.

Bei einer Tätigkeit im Home-Office ist neben dem Arbeitszeitvolumen auch die Lage der Arbeitszeit zu regeln, insbesondere wenn Sie zu bestimmten Zeiten Zugriff auf die Arbeitsleistung Ihrer Mitarbeiter nehmen wollen.

- ***Arbeitsmittel und Kostenerstattung***

Der Arbeitgeber hat grundsätzlich die für die Arbeitstätigkeit erforderlichen Betriebsmittel zu stellen. Das kann zum einen heißen, dass er Mobiliar und Hardware anschafft und dem Arbeitnehmer zur Verfügung stellt. Das kann aber auch bedeuten, dass er sich lediglich an den Kosten für Miete, Strom- und Heizkosten und Mobiliar beteiligt. Letzteres ist eher üblich in Form der Zahlung einer monatlichen Pauschale. Der Grundsatz der Kostentragung gilt selbst dann, wenn, wie in der IT-Branche, Arbeitnehmer vermehrt ihre Hardware selbst stellen („bring your own device" – BYOD). Ob und inwieweit BYOD im Betrieb sinnvoll und zulässig gestaltet werden kann, ist unabhängig davon auch datenschutzrechtlich zu bewerten (s.u.).

Praxistipp: Aus diesem Grund empfehlen wir Arbeitgebern dringend, mit ihren Mitarbeitern eine Kostenpauschale zu vereinbaren.

Ist das Home-Office sogar der einzige vertraglich vereinbarte Arbeitsort des Mitarbeiters, hat dies auch Auswirkungen auf Reisespesen. In diesem Fall tritt Ihr Mitarbeiter bereits dann eine Dienstreise an, sobald er seine Wohnung verlässt. Dies gilt nicht nur für Termine bei Geschäftspartnern, sondern auch für jede einzelne Reise zum Betrieb, beispielsweise um dort an Besprechungen teilzunehmen.

Praxistipp: In diesen Fällen empfehlen wir Ihnen als Arbeitgeber, mit Ihren Mitarbeitern eine vertragliche Kostenregelung zu Dienstreisen zu vereinbaren.

Bei wechselnder Tätigkeit (z.B. drei Wochentage im Home-Office und zwei Wochentage im Büro) muss der Arbeitnehmer dagegen die Kosten für die Fahrt zum Betrieb grundsätzlich selbst tragen.

- ***Arbeitsschutz***

Besonders kritisch ist für Sie als Arbeitgeber das Thema Sicherheit am Arbeitsplatz und Home-Office. Das Arbeitsschutzgesetz und die Arbeitsstättenverordnung gelten grundsätzlich sowohl im Betrieb als auch im Home-Office. Dabei spielt es allerdings eine Rolle, ob das Home-Office vom Arbeitgeber mit Mobiliar ausgestattet wurde oder nicht. Im Falle einer Ausstattung mit Mobiliar (Schreibtisch, Stuhl, Schränke) liegt ein Telearbeitsplatz i.S.d. Arbeitsstättenverordnung vor. Dann muss eine formelle Gefährdungsbeurteilung nach § 3 ArbStättV durchgeführt werden. Ist dem Arbeitnehmer lediglich gestattet, in gewissem Umfang im Home-Office zu arbeiten und stellt der Arbeitgeber nicht die Büroausstattung, liegt kein Telearbeitsplatz vor. Dann fällt auch die formelle Gefährdungsbeurteilung fort. Dennoch folgt aus der Fürsorgepflicht des Arbeitgebers, dass er die Arbeit so gestalten und überprüfen muss, dass eine Gefährdung für das Leben sowie die Gesundheit möglichst vermieden und die verbleibende Gefährdung möglichst geringgehalten wird. Der Arbeitgeber sollte sich also vom Arbeitnehmer zu-

mindest beschreiben lassen, wie sein Home-Office ausgestaltet ist, so dass er bewerten kann, ob Gefährdungen vorliegen könnten.

Wird dagegen ein veritabler Telearbeitsplatz eingerichtet, bei dem der Arbeitgeber die Ausstattung übernimmt, sind Sicherheitsvorschriften einzuhalten, die mitunter sehr detailliert sind (flimmerfreier Monitor, kippsichere Schreibtischstühle). Ihre Mitarbeiter sind verpflichtet, hieran mitzuwirken. Auch aus diesem Grund sollten Sie sich in der Zusatzvereinbarung vertraglich ein Zutrittsrecht zur Wohnung ausbedingen (s.o.).

- ***Laufzeit und Beendigung („Exit-Strategie")***

Wenn Sie mit Ihren Mitarbeitern Home-Office vereinbaren, sollten Sie am besten gleich mitregeln, ob und wie Sie die Vereinbarung wieder beenden können.

Zunächst bietet es sich an, eine befristete Vereinbarung mit Ihren Mitarbeitern zu schließen. Hierbei sollte auf einen sachlichen Grund zur Befristung geachtet werden. Auch bei einer unbefristeten Vereinbarung empfehlen wir Ihnen dringend, sich ein Widerrufsrecht vertraglich vorzubehalten. Dabei muss darauf geachtet werden, dass der Mitarbeiter erkennen kann, „was auf ihn zukommt", d.h., wann er mit einem Widerruf rechnen muss. Fehlt es an einer Widerrufsmöglichkeit und Sie können sich mit Ihrem Mitarbeiter nicht auf eine Beendigung einigen, bleibt Ihnen nur die Möglichkeit, eine Änderungskündigung auszusprechen, die ggf. schwer zu rechtfertigen ist. Nutzen Sie aktuell die Situation, in der Ihre Mitarbeiter im Home-Office arbeiten wollen, um Regeln zu vereinbaren, mit denen Sie auch nach der Corona-Krise leben können.

Auch auf IT-Seite sollte der „Post-Corona"-Zustand bereits mitgedacht werden. Wie kann z.B. sichergestellt werden, dass alle Unterlagen in privaten Räumlichkeiten und Daten auf ggf. privaten Systemen wieder in den unmittelbaren Herrschaftsbereich des Unternehmens gelangen oder DSGVO-konform vernichtet bzw. gelöscht werden (einschließlich Cache, Log-Dateien, Browserverläufen)?

Was ist im Hinblick auf den Datenschutz und die IT-Sicherheit zu beachten?

Der flächendeckende Einsatz von Home-Office ist eine Herausforderung für die Datensicherheit und die Vertraulichkeit der betrieblichen Kommunikation. Dabei gilt es insbesondere, die Anforderungen der DSGVO, des Geheimnisschutzes sowie der allgemeinen Cybersicherheit zu erfüllen. Um die Verhaltensregeln für die Mitarbeiter transparent darzustellen, empfehlen sich eine Home-Office-Richtlinie sowie zusätzliche TOM (technische und organisatorische Maßnahmen), welche ggf. mit der Zusatzvereinbarung zum Arbeitsvertrag verknüpft werden können.

Dort sind insbesondere die folgenden Themen zu regeln:

- ***Welche Hardware ist erlaubt?***

Idealerweise sollten nur betriebliche Laptops, Smartphones etc. eingesetzt werden (vor allem dann, wenn es um sensible Daten bspw. aus dem Personalbereich geht). Dienstliche und private Kommunikation sind grundsätzlich strikt zu trennen. Sofern

der Einsatz von Privatgeräten (BYOD) unumgänglich ist, sollten abgekapselte Bereiche auf Privatgeräten vorgesehen werden.

- ***Wie darf sich der Mitarbeiter mit dem Unternehmensnetzwerk verbinden?***

Ein VPN-Zugriff sollte Standard sein (idealerweise in Kombination mit einer Zwei-Faktor-Authentifizierung). Ebenso eine aktuelle Antiviren-Software und eine aktivierte Firewall. Nicht zuletzt sollte das Netzwerk des Mitarbeiters (meist WLAN) hinreichend geschützt sind.

- ***Wie können Hardware, sonstige Betriebsmittel und Unterlagen effektiv geschützt werden?***

Beispielsweise durch: PIN-/Passwort-Schutz, Festplatten-Verschlüsselung, geschützte Arbeitsbereiche, abschließbare Aktenaufbewahrung.

- ***Wie dürfen und sollen Mitarbeiter intern und extern kommunizieren?***

Kommunikationskanäle und entsprechende Tools sind abschließend zu definieren. Die Privatnutzung von Telefon oder Smartphone muss die Ausnahme bleiben und mit weiteren Maßnahmen einhergehen (z.B. Löschung der Anruflisten, Anonymisierung der Anrufernummer). Der Arbeitgeber hat Tools zu definieren, die eine sichere Kommunikation ermöglichen (z.B. Messenger und Videotelefonie).[1] Das Ausweichen auf „Schatten-IT" (Dropbox, WhatsApp etc.) ist in jedem Fall zu vermeiden.

Thema Video-Kollaboration: Viele Mandanten überlegen sich aktuell, welches Video-Meeting-Tool zulässigerweise eingesetzt werden kann – Zoom? Teams? Skype? WebEx? Der baden-württembergische Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) hat eine aus unserer Sicht sehr restriktive Liste an Empfehlungen zu Videokonferenz-Diensten veröffentlicht. Wir halten jedoch auch bestimmte andere Services kommerzieller Anbieter mit Restrisiken für datenschutzkonform einsetzbar.

- ***Daneben sind weitere Maßnahmen zu ergreifen, z.B.:***
  - Insbesondere bei sensiblen Systemen sollte eine (ohnehin erforderliche) Abschichtung der Zugriffsberechtigten erfolgen („need to know"-Prinzip). Sofern sensible Daten (z.B. Personalakten) auf Endgeräten lokal gespeichert werden müssen, ist eine Verschlüsselung sicherzustellen, z.B. auf einem gesondert verschlüsselten USB-Stick.
  - Regelmäßige Warnungen vor Phishing-Mails oder weiteren Angriffsszenarien, die gerade die wachsende Unsicherheit in Pandemiezeiten ausnutzen wollen („CEO Trick").[2]
  - Unverzügliches Melden des Verlusts von Hardware oder betrieblicher Unterlagen oder des unbefugten Zugriffs hierauf (Meldepflicht nach Art. 33, 34 DSGVO prüfen!).

[1] https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/

[2] Vgl. Warnungen des BSI: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2020/Cyber-Kriminell_02042020.html

- Aufstellen von Notfallplänen und Eskalationsprozeduren für Security Incidents und Data Breaches.
- Gewährleistung regelmäßiger Backups auch von Remote-Geräten.
- Beachtung der „kleinen" Tipps und Tricks, die vielleicht in der „Prä-Corona"-Zeit etwas vernachlässigt wurden, z.B.: Sichtschutzfolien, automatische Bildschirmsperre, Browser-Add-ons, Mail-Anhang-Policy etc.

Diese Maßnahmen sollten in spezifischen sog. Home-Office-TOM[3] zusammengefasst werden, die auch Bestandteil der Home-Office-Richtlinie sein können. Nach Art. 32 DSGVO ist bei allen Maßnahmen dem Stand der Technik Rechnung zu tragen.

- ***Was ist mit Auftragsverarbeitungsverträgen, Verarbeitungsverzeichnissen und Datenschutzhinweisen?***

Denken Sie daran, dass auch Ihre Dienstleister sich höchstwahrscheinlich überwiegend im Home-Office befinden (insbesondere IT-Support-Mitarbeiter und Entwickler-Teams). Klären Sie auch mit diesen unverzüglich die Einhaltung der Home-Office-TOM und die sonstigen Rahmenbedingungen ab. Eine Zusatzvereinbarung, bspw. zu einer bestehenden Vereinbarung zur Auftragsverarbeitung (AVV), kann sich anbieten.

Neu hinzukommende oder geänderte Datenverarbeitungen sind auch im unternehmensinternen Verzeichnis von Verarbeitungstätigkeiten (VVT) nachzuhalten.

Wenn nun etwa ein neues Videokonferenz-Tool eingesetzt wird, betreffen die damit einhergehenden Änderungen an der Datenverarbeitung auch die Endnutzer als betroffene Personen. Um die Informationspflicht aus Art. 13, 14 DSGVO gegenüber Beschäftigten und Ansprechpartnern von Kunden, Lieferanten und sonstigen Geschäftspartnern zu erfüllen, sind entsprechende Datenschutzhinweise (z.B. „Datenschutzerklärung zum Einsatz von MS Teams") vorzusehen.

Und wie setze ich all das in die Tat um?

Veranstalten Sie (virtuelle) Schulungen z.B. in Form interner Webinare, welche die arbeitsrechtlichen Rahmenbedingungen erläutern, über die gesteigerten Cybersicherheits- und Datenschutz-Risiken im Home-Office aufklären sowie die Verhaltensregeln der Home-Office-Richtlinie näherbringen.

Verstärken Sie den IT-Support, der sowohl auf Anfrage von Mitarbeitern, als auch präventiv (z.B. durch Einsatz von Monitoring-Tools) Vorfälle erkennen und diesen nachgehen sollte. Im Fall des Security Monitoring sind natürlich wiederum arbeits- und datenschutzrechtliche Fragen zum zulässigen Einsatz solcher Tools, die auch zur Überwachung der Mitarbeiter dienen können, zu beachten.

Da die IT-Infrastruktur unter Umständen nicht für einen länger andauernden, flächendeckenden Home-Office-Einsatz aus-

[3] Für eine Vertiefung empfehlen wir u.a. die Hinweise der Datenschutzaufsichtsbehörden, des BSI und der ENISA: https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf?__blob=publicationFile und https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely

gelegt ist, sollte parallel zum laufenden Home-Office-Betrieb IT-seitig an einer kontinuierlichen „Härtung" der Systeme gearbeitet werden, um die gesteigerten Risiken auch mit u.U. geringerer personeller Besetzung „abfedern" zu können. Vor allem die Einspielung sicherheitsrelevanter Patches und Updates muss auch „von remote" aus sichergestellt sein.

Beteiligen Sie ggf. Ihren Betriebsrat und betrieblichen Datenschutzbeauftragten.

Unsere Zusammenfassung kann leider nicht alle zur Zeit aufkommenden Themen behandeln. Kommen Sie mit konkreten Fragen, die Sie umtreiben, gerne direkt auf uns zu.

Dr. Roman Frik, LL.M.
Rechtsanwalt
Fachanwalt für Arbeitsrecht
rf@vogel-partner.eu

Stefan Geppert
Rechtsanwalt
sg@vogel-partner.eu

Dr. Uwe K. Schneider
Rechtsanwalt
Fachanwalt für IT-Recht
Fachanwalt für Medizinrecht
us@vogel-partner.eu

Björn Früh
Rechtsanwalt
Certified Information Privacy
Professional Europe (CIPP/E)
bf@vogel-partner.eu